ÜBER GEGEN EINANDER

PERMUTABLE SUBSTITUTIONEN

VON

MARIA ALEXANDER V. BARANIECKI.

INAUGURAL-DISSERTATION

ZUR

ERLANGUNG DER PHILOSOPHISCHEN DOCTOR-WÜRDE

AN DER UNIVERSITÄT LEIPZIG.

LEIPZIG,

DRUCK VON METZGER & WITTIG.

1871.

In den nachstehenden Zeilen wird der Beweis geführt werden, dass die von Cauchy und Serret aufgestellten Formeln und Regeln für Substitutionen, welche gegen einander permutabel sind, nicht allgemein (wie die genannten Gelehrten behaupten), sondern nur für einen Specialfall gültig sind (§§ II u. III). Hieran wird sich die Aufstellung von solchen Formeln knüpfen, aus denen sich die obenerwähnten als Specialfälle ergeben (§ IV).

Der Vollständigkeit halber mögen in § I einige Hauptdefinitionen Platz finden. Wir werden sodann einen systematischen Beweis der Behauptung aufstellen, dass die Bildung einer, gegen eine gegebene, permutablen Substitution auf die Aufsuchung von Specialsubstitutionen hinauskommt, die durch cyclische Versetzung einer gewissen Anzahl von Cyclen derselben Ordnung entstehen.

Es mag hierbei noch erwähnt werden, dass C. Jordan in seinem unlängst erschienen Werke „Traité des substitutions et des équations algébriques." unsere Frage nicht berührt.

Endlich wird der geneigte Leser gebeten, die Schwierigkeiten, welche das deutsche Idiom dem Verfasser bot, bei Beurtheilung dieser Arbeit nachsichtig in Anschlag bringen zu wollen.

Leipzig, am 4. Mai 1871.

§ I.

1. Sind zwei Substitutionen so beschaffen, dass sie bei Ausführung der ersten nach der zweiten, oder dieser nach jener, dasselbe Resultat liefern, so heissen sie gegen einander permutabel, oder kürzer, permutable Substitutionen.

Irgend zwei derartige Substitutionen mögen mit dem Buchstaben S und T bezeichnet werden; wir werden dann die Eigenschaft derselben symbolisch durch die Lineargleichung

$$ST = TS \tag{1}$$

darstellen können.

Besitzen die Substitutionen S und T kein gemeinschaftliches Element, so genügen sie der Relation (1) selbstverständlich. Es wird daher unsere Aufgabe sein, solche Substitutionen ausfindig zu machen, welche der Gleichung (1) genügen und dabei nur gemeinschaftliche Elemente besitzen. Sollten nämlich Substitutionen auftreten, die einige gemeinschaftliche und daneben solche Elemente enthalten, welche nur in der einen Substitution vorkommen, so können wir annehmen, dass diese letzteren Elemente auch in der anderen Substitution als Circularfactoren erster Ordnung vorhanden sind und sie zum Vorschein bringen. Wir haben also nur darzulegen, auf welche Weise aus einer gegebenen Substitution alle gegen dieselbe permutablen und dieselben Elemente, wie die gegebene, enthaltenden Substitutionen abgeleitet werden können, oder allgemeiner die Bedingung anzugeben, welcher die beiden, ausschliesslich gemeinschaftliche Elemente besitzenden, permutablen Substitutionen S und T genügen.

2. Vermöge der Relation (1) hat man

$$S = TST^{-1}, \tag{2}$$

woraus folgt, dass die Substitution S dieselbe bleibt, sobald man sie durch Weglassung der Klammern und Kommata in eine Complexion verwandelt und in dieser die Substitution T ausführt. Es kann da-

her die Substitution T in S nur eine Veränderung der Form hervorbringen.

Jede Substitution darf als das Product mehrer regelmässigen Substitutionen betrachtet werden. Sodann kann man alle möglichen Formen dieser Substitution ohne Veränderung ihrer Bedeutung bilden, so zwar, dass man die Cyclen derselben Ordnung gegen einander versetzt und in jedem Cyclus jedes Element, bei übrigens gleicher cyclischer Aufeinanderfolge der Elemente des Cyclus, an die erste Stelle bringt. Hat die Substitution S m Cyclen von der Ordnung n, m_1 Cyclen von der Ordnung n_1 etc., so wird man als Resultat aller Translocationen der Cyclen,

$$1.2.3\ldots m.1.2.3\ldots m_1\ldots$$

Formen erhalten. Indem nun in jedem Cyclus jeder Form jedes Element an die erste Stelle gebracht wird, ergiebt sich die Zahl

$$1.2.3\ldots m.1.2.3\ldots m_1\ldots n^m n_1^{m_1}\ldots,$$

als Betrag aller verschiedenen Formen der Substitution S.

Nimmt man in der Relation (2) auf der rechten Seite immer dieselbe Form der Substitution S, so wird man die verschiedenen Formen der anderen Seite abhängig von der Substitution T erhalten. Sind dann in zwei solchen Relationen wie (2) die Substitutionen T (in irgend welchen Formen) dieselben, so werden auf der linken Seite keine davon verschiedenen Formen der Substitution S hervorgehen. Die Anzahl der verschiedenen Substitutionen T, welche der Relation (1) genügen, wird sonach mit der Anzahl der Formen der Substitution S übereinstimmen.

3. Sei S eine gegebene Substitution. Nachdem man in derselben alle Elemente zum Vorschein gebracht hat, ergiebt selbige sich als das Product mehrer regelmässigen Substitutionen

$$S = PP_1P_2\ldots,$$

von denen jede zusammengesetzt ist aus

$$m,\ m_1,\ m_2,\ldots$$

Cyclen von der resp. Ordnung

$$n,\ n_1,\ n_2,\ldots.$$

Schreibt man über die Substitution S eine andere Form derselben, so erhält man eine neue Substitution, welche man nach der Theorie der ähnlichen Substitutionen für T zu nehmen hat, um die lineare und symbolische Gleichung (1) aufzulösen, d. h. um eine gegen S permutable Substitution zu bestimmen. Hieraus schliesst man: 1^0, dass, was man auch für eine Form für S als untere Zeile nehmen mag, doch immer die Anzahl der Werthe von T dieselbe

bleibt und dass die Werthe nur in verschiedener Aufeinanderfolge auftreten; 2°, dass die Veränderungen, mit deren Hilfe man die verschiedenen Formen der Substitution S erhält, bei den regelmässigen Substitutionen allein stattfinden, dergestalt, dass eine Veränderung, welche man in einer der Substitutionen

$$P, P_1, P_2, \ldots \tag{3}$$

vornimmt, in den Werthen für T keinen Einfluss auf diejenigen Theile hat, welche von anderen regelmässigen Substitutionen von S gebildet sind. Es folgt daraus weiter, dass die gefundenen Werthe von T als die Producte mehrer partiellen Substitutionen

$$T = QQ_1Q_2 \ldots \tag{4}$$

dargestellt werden können, von denen jede aus einer der Substitutionen (3) gebildet und gegen dieselbe permutabel wird. Man sieht also, dass die Aufsuchung der Werthe (4), welche der Relation (1) genügen, die Bestimmung der einfachen Substitutionen

$$Q, Q_1, Q_2, \ldots,$$

deren jede gegen die entsprechende in (3) permutabel ist, erfordert.

4. Da die Substitution P aus m Cyclen zusammengesetzt ist, so wird die Anzahl der Werthe von Q, welche der Relation

$$PQ = QP$$

genügen, gleich der Anzahl der Formen von P, d. h. gleich

$$1.2.3 \ldots m n^m$$

sein.

Man wird nämlich diese Formen erhalten, wenn man m cyclische Versetzungen von allen m Cyclen ausführt, hierauf in jeder dieser Formen, nach Weglassung eines Cyclus, z. B. des letzten, alle $m-1$ cyclischen Versetzungen der $m-1$ bleibenden Cyclen bildet, alsdann wieder in jeder solcher neu entstandenen Form noch den zweiten Cyclus, z. B. den vorletzten weglässt, alle $m-2$ cyclischen Versetzungen mit $m-2$ Cyclen vornimmt und dies Verfahren fortsetzt, bis alle Formen von P gebildet sind. Aus jeder von diesen

$$1.2.3 \ldots m$$

Formen entstehen n^m, wenn man in dem ersten Cyclus jedes von seinen n Elementen an die erste Stelle setzt und später in den auf diese Weise erhaltenen Formen im zweiten Cyclus dasselbe Verfahren wiederholt etc.

Durch diese letzteren Veränderungen ergeben sich über einem Cyclus seine anderen Formen; es wird daher in der Substitution Q eine der n Potenzen dieses Circularfactors vorkommen.

Was die cyclischen Versetzungen der Cyclen betrifft, so brauchen diese nicht immer eine cyclische Versetzung von allen Cyclen zu bilden. Denn es wird die Translocation der Cyclen z. B. durch eine cyclische Versetzung von μ Cyclen unter der Annahme gebildet, dass eine Form der Substitution P entsteht, indem man ausführt: m cyclische Versetzungen von m Cyclen (dabei werden die Cyclen an ihrer Stelle bleiben), $m-1$ cyclische Versetzungen von $m-1$ Cyclen (was ebenfalls die Stellung der Cyclen nicht verändert) etc., $\mu+1$ cyclische Versetzungen von $\mu+1$ Cyclen, eine einzige cyclische Versetzung von μ Cyclen und endlich $\mu-1, \mu-2, \ldots, 3, 2$ cyclische Versetzungen von resp. derselben Anzahl der Cyclen. — Aus dieser so erhaltenen Form können durch Vertauschung der ersten Elemente in den Cyclen alle n^m Formen reproducirt werden. Man erhält nämlich auf diese Weise aus μ translocirten Cyclen n^μ Formen. Aus jeder dieser Formen entspringen $n^{m-\mu}$, weil jeder von den $m-\mu$ Cyclen, die nicht versetzt und die, als Elemente angesehen, Cyclen erster Ordnung bilden, durch Einführung eines jeden von seinen Elementen in die erste Stelle, n Formen giebt. Alle $m-\mu$ Cyclen liefern $n^{m-\mu}$ Formen; im Ganzen hat man daher n^m.

Es folgt hieraus, dass in der Anzahl der

$$1.2.3\ldots m$$

Formen, jede Form der Substitution P, welche durch irgend eine cyclische Versetzung von beliebigen Cyclen entstanden ist, sich vorfinden wird. Als ein specieller Fall kann die Substitution Q gleich dem Producte der Cyclen erster Ordnung zum Vorschein kommen und dann wird

$$Q = 1.$$

5. Lässt sich eine Substitution P infolge einer zwischen ihren Cyclen stattgefundenen Translocation nur mit Hilfe von zwei oder mehreren cyclischen Versetzungen (oder deren Potenz), welche sich auch auf gemeinschaftliche Elemente und auf eine verschiedene Anzahl von Cyclen beziehen, ausdrücken, so werden sich auf Grund des Vorhergehenden, in der Anzahl aller Formen auch Formen der Substitution P vorfinden, die aus diesen einzelnen cyclischen Versetzungen entstanden sind und die wir hier der Reihe nach auszuführen haben. Indem wir nun eine von diesen Formen über die gegebene schreiben, erhalten wir einen von den Werthen Q, welcher eine gegen P permutable Substitution bildet. Sind mehrere Substitutionen gegen eine andere permutabel, so ist der Behauptung von Cauchy*) gemäss auch ihr Product gegen diese Substitution permu-

*) „Exercices d'analyse et de physique mathématique." Tome III. p. 224. (Auch bei J. A. Serret in „Cours d'algèbre supérieure." Tome II. n⁰. 408. 3ème éd.)

tabel. Es folgt daraus, dass das Product aller Werthe Q gegen die Substitution P permutabel ist, so dass wir unsere Aufgabe lösen können, indem wir für jede cyclische Versetzung, oder ihre Potenz, den entsprechenden in dem gesuchten Werthe Q inbegriffenen Factor bestimmen und das Product dieser Factoren der Reihe nach nehmen.

6. Haben wir zur Bestimmung eines Werthes Q die cyclische Versetzung von Cyclen in einer Potenz, die zu der Zahl der versetzten Cyclen nicht prim ist, auszuführen, so zerfällt die Versetzung der Cyclen in mehrere gleichzeitige, mit keinem gemeinschaftlichen Element versehene cyclische Versetzungen. Ist allgemein die Form der Substitution P in der oberen Zeile so beschaffen, dass sie als das Resultat der Potenv η einer cyclischen Versetzung von μ Cyclen erscheint, so wird im Falle η zu μ prim ist, die Translocation der Cyclen durch die erste Potenz einer anderen cyclischen Versetzung ausgedrückt. Wenn aber η ein Divisor von μ ist, oder allgemeiner gesagt, mit μ den grössten gemeinschaftlichen Divisor ι hat, dann erhalten wir für Q einen Werth, welcher aus ι simultanen, keine gemeinschaftlichen Elemente besitzenden Substitutionen zusammengesetzt ist. Letztere sind daher aus $\frac{\mu}{\iota}$ verschiedenen Cyclen der Substitution P entstanden und sowohl gegen einander, als auch gegen die Substitution P permutabel. Wir sehen also, dass auch dieser Fall sich auf die Aufsuchung der gegen P permutablen, aus einfacher Circular-Translocation der Cyclen entstandenen Substitutionen reducirt. Wir erhalten hier ein der Voraussetzung entsprechendes Endresultat, indem wir aus allen auf solche Weise erzeugten, in beliebiger Reihe geordneten partiellen Substitutionen ein Product bilden.

§ II.

7. A. L. Cauchy behauptet [cf. „Mémoire sur les substitutions permutables entre elles.“*) — „Mémoire sur les arrangements, que l'on peut former avec des lettres données, et sur les permutations ou substitutions, à l'aide desquelles on passe d'un arrangement à un autre.“ (§ IX. „Des substitions permutables entre elles.“)**)],

*) „Comptes rendus hebdomadaires de l'académie des sciences.“ Tome XXI. (1845.) Nr. 22.

**) „Exercices d'analyse et de physique mathématique.“ Tome III. p. 210—226. Da Cauchy in den beiden Abhandlungen sich nicht ganz gleicher Zeichen bedient, so werden wir uns an das Zeichensystem in „Exercices.“ halten, da dieses uns systematischer als das in den „Comptes rendus.“ erscheint.

dass jede Substitution als ein Product mehrerer regelmässigen Substitutionen

$$P = \mathfrak{P}\mathfrak{P}'\mathfrak{P}''\ldots$$

angesehen werden könne. Zunächst betrachtet er den Fall, bei welchem die Substitution regelmässig und aus h Cyclen von der Ordnung a

$$P = \mathfrak{P} = \mathfrak{R}\mathfrak{S}\mathfrak{T}\ldots$$

zusammengesetzt ist.

Durch Ausführung der cyclischen Substitution

$$(\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots),$$

erhält er als den ersten Cyclus einer gegen P permutablen Substitution Q, welche der linearen und symbolischen Gleichung

$$QP = PQ$$

genügt, folgende cyclische Substitution

(5) $$(\alpha, \beta, \gamma, \ldots, \lambda, \mu, \nu, \ldots, \varphi, \chi, \psi, \ldots, \ldots).$$

Die Elemente dieser cyclischen Substitution lassen sich durch die Tafel

(6) $$\begin{cases} \alpha, \ \beta, \ \gamma, \ \ldots \\ \lambda, \ \mu, \ \nu, \ \ldots \\ \varphi, \ \chi, \ \psi, \ \ldots \\ \quad \text{etc.} \end{cases}$$

ausdrücken. In dieser Tafel sind alle ersten Elemente der horizontalen Reihen aus $\mathfrak{R}$, alle zweiten aus $\mathfrak{S}$, alle dritten aus $\mathfrak{T}$ etc. genommen. Wenn wir die Anzahl der horizontalen Reihen mit θ bezeichnen, so wird die Anzahl b aller Elemente in (5) den Werth

$$b = \theta h$$

besitzen.

Alle Elemente, welche sich in den entsprechenden Cyclen der Substitution P auf den nächstfolgenden Stellen befinden, bilden einen zweiten Cyclus der Substitution Q

$$(\alpha', \beta', \gamma', \ldots, \lambda', \mu', \nu', \ldots, \varphi', \chi', \psi', \ldots, \ldots),$$

und zwar ebenfalls von der Ordnung

$$b = \theta h;$$

die darauf folgende bilden den dritten Cyclus u. s. f.

8. Sehen wir jetzt zu, in welchem Falle die zweite Reihe, sowie die folgenden Reihen der Tafel (6) vorkommen können, d. h. unter welcher Bedingung θ von 1 verschieden sein und einen der Werthe

$$\delta', \delta'', \ldots, a$$

annehmen kann, wobei

$$\delta, \delta'', \ldots$$

die Divisoren der Zahl a sind.

Unter den Zeichen

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

verstehen wir cyclische Substitutionen von allen a Formen, durch welche wir sie mittelst Einführung jedes Elementes in die erste Stelle darstellen können. Wenn die Substitution

$$(\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots)$$

in der gegebenen und der neuentstandenen Complexion in den durch Weglassung der Klammern und Kommata aus den entsprechenden Cyclen entstandenen Theilen einerlei Anfangselemente besitzt, d. h. wenn in der Substitution

$$\begin{pmatrix} \mathfrak{S}\mathfrak{T}\ldots\mathfrak{R} \\ \mathfrak{R}\mathfrak{S}\mathfrak{T}\ldots \end{pmatrix} \tag{7}$$

die entsprechenden Theile der Complexionen, welche wir hier durch das Zeichen desselben Circularfactors z. B. $\mathfrak{T}$ ausgedrückt haben, sowohl in den oberen wie auch in den unteren Zeilen aus derselben Form entstanden sind, dann wird das zweite Element des Cyclus der Substitution Q, welches in (7) in der oberen Zeile auf der Stelle ζ war, in der unteren Zeile offenbar auf der $\zeta + a$-ten stehen, und das, auf der Stelle $\zeta + a$ der oberen Zeile befindliche Element in der unteren Zeile auf der $\zeta + 2a$-ten vorkommen u. s. w., schliesslich wird das Element, welches in der oberen Zeile die Stelle $\zeta + (h - 2)a$ und in der unteren $\zeta + (h-1)a$ einnahm, über sich dasjenige Element haben, welches, bei Anordnung der Elemente am Umfange eines Kreises, in der unteren Zeile auf der Stelle $\zeta + ah$ vorkommen soll. Da aber die Anzahl aller Elemente ah beträgt und da

$$\zeta + ah \equiv \zeta \pmod{ah},$$

so ist dieses letzte Element dasselbe, welches in (7) in der unteren Zeile die Stelle ζ einnimmt, d. h. dasselbe Element, von welchem wir ausgegangen sind; somit ist der Cyclus geschlossen. Hieraus folgt, dass, wenn jeder von den Cyclen

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

in derselben Form zur Bildung der unteren und der oberen Zeile der Substitution (7) genommen wird, nothwendig

$$\theta = 1$$

ist.

Jeder von den Cyclen der Substitution Q wird also ein einziges Element aus jedem Cyclus der Substitution P enthalten, und die zweite, sowie die folgenden Reihen werden in der Tafel (6) nicht vorkommen.

9. Damit die Gleichheit

$$b = h$$

nicht stattfinde, ist es durchaus nöthig, obgleich, wie wir später sehen werden, nicht hinreichend, dass in (7) nicht alle Cyclen der oberen Zeile mit denselben Elementen wie die entsprechenden Cyclen der unteren Zeile beginnen.

Betrachten wir zuerst den Fall, dass aus

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

nur ein Cyclus z. B. $\mathfrak{T}$, den wir, um die Sache zu verallgemeinern, als den t^{ten} der unteren Zeile ansehen, mit einem anderen Elemente in der oberen, als in der unteren Zeile anfängt. Bezeichnen wir durch $\mathfrak{T}_{(\tau)}$ diejenige Form des Cyclus $\mathfrak{T}$, deren erstes Element als Index die in der Reihe

$$0, 1, 2, \ldots, a-2, a-1$$

an der Stelle $\tau + 1$ vorhandene Zahl hat, so wird, wenn diese Form in der einen Zeile vorkommt, in der andern eine von den folgenden Formen

$$\mathfrak{T}_{(\tau+1)}, \mathfrak{T}_{(\tau+2)}, \ldots, \mathfrak{T}_{(a-1)}, \mathfrak{T}_{(0)}, \mathfrak{T}_{(1)}, \ldots, \mathfrak{T}_{(\tau-1)}$$

auftreten. Wir wollen hier annehmen, dass $\mathfrak{T}_{(\tau_0)}$ und $\mathfrak{T}_{(\tau_1)}$, $\tau_0 \lessgtr \tau_1$, die Formen der unteren und der oberen Zeile sind und dass

$$\tau_1 - \tau_0 = \pi_\tau\,; \quad \pi_\tau \lessgtr 0.$$

Da hier alle Cyclen vor $\mathfrak{T}$ in beiden Theilen einförmig sind, so nehmen wir, um den ζ^{ten} Cyclus der Substitution Q zu bilden, die Elemente aus den Stellen

$$\zeta, \zeta + a, \zeta + 2a, \ldots, \zeta + (t-1)a$$

der unteren Zeile. Dasjenige Element des Cyclus $\mathfrak{T}$, welches in der oberen Zeile auf der Stelle $\zeta + (t-1)a$ war, wird in der unteren Zeile auf der Stelle

$$\zeta + \pi_\tau + ta \tag{8}$$

vorkommen, wobei wir unter $\zeta + \pi_\tau + ta$ die Zahl zwischen ta und $(t+1)a$ verstehen. Ist aber

$$\zeta + \pi_\tau + ta > (t+1)a, \text{ oder } < ta,$$

d. h.

$$\zeta + \pi_\tau > a, \text{ oder } < 0,$$

so hat man in (8) unter $\zeta + \pi_\tau$ den kleinsten positiven Rest dieser Zahl nach dem Modul a zu verstehen. Da die folgenden Cyclen einförmig sind, so stammen die Elemente, welche wir aus diesen Cyclen nehmen sollen, nebst den früher genommenen Elementen, aus den Stellen

$$\zeta, \zeta+a, \ldots, \zeta+(t-1)a, \zeta+\pi_\tau+ta, \zeta+\pi_\tau+(t+1)a, \ldots, \zeta+\pi_\tau+(h-1)a$$

der unteren Zeile. Ueber dem zuletzgenommenen Elemente figurirt in der oberen Zeile ein Element aus der Stelle $\zeta + \pi_\tau + (h-1)a$, welches sich, als dem einförmigen Cyclus angehörend, bei der Anordnung der Elemente am Umfange eines Kreises, auf der Stelle $\zeta + \pi_\tau + ah$, d. h. $\zeta + \pi_\tau$ befindet. Da π_τ kleiner als a ist, folglich auch kein Multiplum von a sein kann, ferner nach unserer Annahme von Null verschieden ist, so findet die Relation

$$\zeta + \pi_\tau \equiv (\text{mod } a)$$

nicht statt, d. d. wir sind nicht auf dasselbe Element gekommen, und der Cyclus ist nicht geschlossen. Als folgende Elemente werden wir diejenigen nehmen, welche auf den Stellen

$$\zeta + \pi_\tau, \zeta + \pi_\tau + a, \ldots, \zeta + \pi_\tau + (t-1)a, \zeta + 2\pi_\tau + ta, \ldots, \zeta + 2\pi_\tau + (h-1)a$$

der unteren Zeile sich befanden, indem wir hier unter $\zeta + 2\pi_\tau$, ähnlich wie in (8), den kleinsten positiven Rest nach dem Modul a verstehen. Wenn das Element, welches in der oberen Zeile an der Stelle $\zeta + 2\pi_\tau + (h-1)a$ vorkommt, nicht dasjenige ist, welches in der unteren Zeile auf der Stelle ζ war, d. h. wenn die Congruenz

$$\zeta + 2\pi_\tau \equiv (\text{mod } a)$$

nicht stattfindet, so werden wir weiter Elemente der Substitution (7) so lange nehmen, bis wir, nachdem wir die Elemente aus den Stellen

$$\zeta + (\theta-1)\pi_\tau, \zeta + (\theta-1)\pi_\tau + a, \ldots, \zeta + \theta\pi_\tau + ta, \ldots, \zeta + \theta\pi_\tau + (h-1)a$$

der unteren Zeile genommen haben [in Betreff der Zahlen

$$\zeta + 3\pi_\tau, \ldots, \zeta + (\theta-1)\pi_\tau, \zeta + \theta\pi_\tau$$

machen wir hier ähnliche Bedingung wie in (8)], auf ein solches Element stossen, welches bei Anordnung der Elemente am Kreisumfange auf der Stelle $\zeta + \theta\pi_\tau + ha$, d. h. $\zeta + \theta\pi_\tau$ der unteren Zeile in (7) sich befindet, wobei die Zahl θ der Congruenz

$$\zeta + \theta\pi_\tau \equiv \zeta \ (\text{mod } a) \tag{9}$$

genügt. Es ist also dann der Cyclus geschlossen.

Aus dieser Congruenz (9) folgt

$$\theta\pi_\tau \equiv 0 \ (\text{mod } a)$$

und daraus entsteht, wenn π_τ und a prim zu einander sind, da π_τ von Null verschieden und nicht grösser als a ist,

$$\theta = a.$$

Wenn aber die Zahlen π_τ und a den grössten gemeinschaftlichen Divisor δ haben, so wird sich die Congruenz (9) in

$$\theta\frac{\pi_\tau}{\delta} \equiv \left(\text{mod } \frac{a}{\delta}\right)$$

verwandeln und aus dieser, da $\frac{\pi_\tau}{\delta}$ zum Modul prim ist, hervorgehen

$$\theta = \frac{a}{\delta}.$$

10. Indem wir im Allgemeinen die Formen der Cyclen

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

der unteren Zeile der Substitution

$$\begin{pmatrix} \mathfrak{S}\mathfrak{T} \ldots \mathfrak{R} \\ \mathfrak{R}\mathfrak{S}\mathfrak{T} \ldots \end{pmatrix}$$

mit

$$\mathfrak{R}_{(\varrho_0)}, \mathfrak{S}_{(\sigma_0)}, \mathfrak{T}_{(\tau_0)}, \ldots$$

und der oberen mit

$$\mathfrak{R}_{(\varrho_1)}, \mathfrak{S}_{(\sigma_1)}, \mathfrak{T}_{(\tau_1)}, \ldots$$

bezeichnen, wobei die Indices

$$\varrho_0, \sigma_0, \tau_0, \ldots; \varrho_1, \sigma_1, \tau_1, \ldots$$

beliebigen Zahlen aus der Reihe

$$0, 1, 2, \ldots, a-2, a-1$$

entsprechen, indem wir ferner

$$\varrho_1 - \varrho_0 = \pi_\varrho, \ \sigma_1 - \sigma_0 = \pi_\sigma, \ \tau_1 - \tau_0 = \pi_\tau, \ldots$$

setzen, ist der Cyclus geschlossen, sobald wir aus jeder partiellen Substitution

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

so viel Elemente nehmen, dass ihre Anzahl θ, die kleinste positive, der Congruenz

(10) $$\theta(\pi_\varrho + \pi_\sigma + \pi_\tau + \ldots) \equiv 0 \pmod{a}$$

genügende Zahl ist. — Man hat

$$\theta = 1,$$

wenn

$$\pi_\varrho + \pi_\sigma + \pi_\tau + \ldots = 0,$$

was möglich ist, wenn entweder (entsprechend dem in Art. 8 discutirten Falle)

$$\pi_\varrho = \pi_\sigma = \pi_\tau = \ldots = 0,$$

oder wenn die Zahlen

$$\pi_\varrho, \pi_\sigma, \pi_\tau, \ldots,$$

gleichen oder verschiedenen Vorzeichens, eine Summe

(11) $$\pi_\varrho + \pi_\sigma + \pi_\tau + \ldots$$

ergeben, die einem der mit positiven oder negativen Vorzeichen versehenen Multipla von a

$$a, 2a, \ldots, (h-1)a$$

gleich ist. Ist die genannte Summe zu a prim, so gilt

$$\theta = a;$$

hat sie aber mit a den grössten gemeinschaftlichen Divisor δ, dann wird

$$\theta = \frac{a}{\delta}.$$

Ertheilt man entweder allen, oder einigen, oder sogar nur einzelnen Zahlen, die zu der Summe (11) gehören, verschiedene Werthe, so wird man für θ alle Divisoren von a erhalten.

Alle diese Fälle können wir auf einen allgemeinen Fall zurückführen und sagen: wenn die Summe (11), resp. ihr kleinster Rest nach dem Modul a, mit a eine von den Zahlen

$$1, \delta', \delta'', \ldots, \frac{a}{\delta'}, a$$

zum grössten gemeinschaftlichen Divisor hat, so ist laut (10)

$$\theta = a, \frac{a}{\delta'}, \frac{a}{\delta''}, \ldots, \delta', 1.$$

11. Gehen wir auf den Fall zurück, den wir in Art. 9 behandelt haben, so wird unter der Voraussetzung

$$\pi_\tau < 0$$

(was jedesmal stattfindet, wenn

$$\tau_1 < \tau_0),$$

das zweite aus dem Cyclus $\mathfrak{R}$ genommene, also das auf der Stelle $\zeta + \pi_\tau$ des Cyclus $\mathfrak{R}$ befindliche Element, in diesem Cyclus auf der linken Seite des bereits genommenen Elementes (welches in diesem Cyclus auf der Stelle ζ stand) vorkommen. — Da nun τ_1 einen beliebigen von den Werthen

$$0, 1, 2, \ldots, \tau_0 - 1, \tau_0 + 1, \ldots, a - 1$$

darstellen kann, so nehmen wir zur Bildung der Substitution Q, die zwei ersten Elemente des Cyclus $\mathfrak{R}$ in einer anderen oder in derselben Ordnung, in der sie sich in $\mathfrak{R}$ befinden, je nachdem

$$\tau_1 < \tau_0, \text{ oder } \tau_1 > \tau_0.$$

Ist nun

$$\tau_1 < \tau_0, \tau_1 > a - \tau_0, 2\tau_1 > a,$$

so nehmen wir als drittes Element des Cyclus $\mathfrak{R}$ das in diesem Cyclus vor dem ersten und zweiten der bereits genommenen Elemente befindliche Element. Indem wir verschiedene derartige Grenzen für τ_1, abhängig von τ_0, bestimmen, können wir aus den zur Bildung des Cyclus der Substitution Q genommenen Elementen des Cyclus $\mathfrak{R}$ gewisse Complexionen erhalten, die von den, durch diese Elemente (dieselben einzeln betrachtet) im Cyclus $\mathfrak{R}$ gebildeten

Complexionen verschieden sein werden. Diese Verschiedenheit ist unabhängig von der in der gegebenen Substitution P als vorkommend gedachten Form des Cyclus $\mathfrak{T}$, denn jede beliebige als Ausgangsform benutzte Form kann als die Form $\mathfrak{T}_{(\tau_0)}$ angesehen werden.

Es wird dasselbe a fortiori stattfinden, wenn wir einen Fall annehmen, der noch allgemeiner ist, als der hier in Betracht gezogene.

Wir sehen also, dass wenn wir bei partiellen cyclischen Substitutionen, von jeder je einige Elemente nach der Reihe

$$\begin{array}{c} \alpha, \lambda, \varphi, \ldots \\ \beta, \mu, \chi, \ldots \\ \gamma, \nu, \psi, \ldots \\ \text{etc.} \end{array}$$

nehmen, es durchaus nicht nöthig ist, dass dieselben sich in derselben Reihenfolge in den entsprechenden Cyclen

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

befinden. Umgekehrt, wenn die Tafel der in dem ersten Cyclus der Substitution Q benutzten Elemente die Reihenfolge bezeichnet, in welcher die Elemente der ersten Zeile im Cyclus $\mathfrak{R}$, der zweiten im Cyclus $\mathfrak{S}$ etc. vorkommen, so ist es nicht unbedingt nothwendig, dass diese Tafel uns gleichzeitig die Reihenfolge der in den Cyclen der Substitution Q befindlichen Elemente angiebt.

Wenn daher

$$Q = \mathfrak{U}\mathfrak{V}\mathfrak{W}\ldots$$

und

$$(12) \qquad \begin{cases} \mathfrak{U} = (\alpha, \beta, \gamma, \ldots, \lambda, \mu, \nu, \ldots, \varphi, \chi, \psi, \ldots, \ldots), \\ \mathfrak{V} = (\alpha', \beta', \gamma', \ldots, \lambda', \mu', \nu', \ldots, \varphi', \chi', \psi', \ldots, \ldots), \\ \text{etc.,} \end{cases}$$

so folgt nicht daraus, dass „— — les variables, qui succéderont les unes aux autres, en vertu du facteur circulaire $\mathfrak{R}$ de la Substitution P, seront évidemment

$$\alpha, \alpha', \alpha'', \ldots, \lambda, \lambda', \lambda'', \ldots, \varphi, \varphi', \varphi'', \ldots, \ldots;$$

pareillement, les variables, qui succéderont les unes aux autres dans le facteur $\mathfrak{S}$ de la Substitution P, seront

$$\beta, \beta', \beta'', \ldots, \mu, \mu', \mu'', \ldots, \lambda, \lambda', \lambda'', \ldots, \ldots,$$

— — etc.“*). Die Cyclen (12) der Substitution Q haben ferner nicht immer zur Folge

$$\begin{cases} \mathfrak{R} = (\alpha, \alpha', \alpha'', \ldots, \lambda, \lambda', \lambda'', \ldots, \varphi, \varphi', \varphi'', \ldots, \ldots), \\ \mathfrak{S} = (\beta, \beta', \beta'', \ldots, \mu, \mu', \mu'', \ldots, \chi, \chi', \chi'', \ldots, \ldots), \\ \text{etc.}^{**}), \end{cases}$$

*) „Exerc.“ p. 213. „Comp. rend.“ p. 1192. **) Ibidem.

was nur in einigen Spezialfällen stattfindet, nämlich, wenn nicht nur

$$\varrho_1 \leqq \varrho_0 + \frac{a}{\theta},\ \sigma_1 \leqq \sigma_0 + \frac{a}{\theta},\ \tau_1 \leqq \tau_0 + \frac{a}{\theta}, \ldots,$$

sondern auch gleichzeitig

$$\pi_\varrho + \pi_\sigma + \pi_\tau + \ldots \equiv \frac{a}{\theta} \pmod{a}.$$

12. Wir wollen das Ergebniss unserer Untersuchung an einem Beispiele erläutern. Gehen wir von der Substitution

$$\mathrm{P} = \mathfrak{R}\mathfrak{S}\mathfrak{T}$$

aus, wo

$$\begin{aligned} \mathfrak{R} &= (\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5), \\ \mathfrak{S} &= (\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5), \\ \mathfrak{T} &= (\gamma_0, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5). \end{aligned}$$

Um nun einen von den Werthen der Substitution Q, der der linearen und symbolischen Gleichung

$$\mathrm{QP} = \mathrm{PQ}$$

Genüge leistet, zu bestimmen, führen wir die Translocation der Cyclen

$$(\mathfrak{R}, \mathfrak{S}, \mathfrak{T})$$

aus, indem wir den Cyclen in den beiden Zeilen dieselben Formen

$$\mathfrak{R}_{(0)}, \mathfrak{S}_{(2)}, \mathfrak{T}_{(5)}$$

geben. Es ist dann

$$\begin{pmatrix} \mathfrak{S}_{(2)} \mathfrak{T}_{(5)} \mathfrak{R}_{(0)} \\ \mathfrak{R}_{(0)} \mathfrak{S}_{(2)} \mathfrak{T}_{(5)} \end{pmatrix} = \begin{pmatrix} \beta_2 \beta_3 \beta_4 \beta_5 \beta_0 \beta_1 & \gamma_5 \gamma_0 \gamma_1 \gamma_2 \gamma_3 \gamma_4 & \alpha_0 \alpha_1 \alpha_2 \alpha_3 \alpha_4 \alpha_5 \\ \alpha_0 \alpha_1 \alpha_2 \alpha_3 \alpha_4 \alpha_5 & \beta_2 \beta_3 \beta_4 \beta_5 \beta_0 \beta_1 & \gamma_5 \gamma_0 \gamma_1 \gamma_2 \gamma_3 \gamma_4 \end{pmatrix}$$

und

$$\mathrm{Q} = (\alpha_0, \beta_2, \gamma_5)(\alpha_1, \beta_3, \gamma_0)(\alpha_2, \beta_4, \gamma_1)(\alpha_3, \beta_5, \gamma_2)(\alpha_4, \beta_0, \gamma_3)(\alpha_5, \beta_1, \gamma_4).$$

Um einen anderen Werth für Q zu bestimmen, geben wir den Cyclen verschiedene Formen. Wir wollen z. B. ausführen

$$\begin{pmatrix} \mathfrak{S}_{(0)} \mathfrak{T}_{(2)} \mathfrak{R}_{(0)} \\ \mathfrak{R}_{(0)} \mathfrak{S}_{(4)} \mathfrak{T}_{(4)} \end{pmatrix}.$$

Hieraus erhält man

$$\mathrm{Q} = (\alpha_0, \beta_0, \gamma_4)(\alpha_1, \beta_2, \gamma_5)(\alpha_2, \beta_2, \gamma_0)(\alpha_3, \beta_3, \gamma_2)(\alpha_4, \beta_4, \gamma_2)(\alpha_5, \beta_5, \gamma_3).$$

Wir hatten hier

$$\pi_\varrho = 0,\ \pi_\sigma = -4,\ \pi_\tau = -2;\ \alpha = 6,$$
$$\pi_\varrho + \pi_\sigma + \pi_\tau \equiv 0 \pmod{6};$$

und daraus folgte

$$\theta = 1.$$

Jetzt nehmen wir z. B.

$$\begin{pmatrix} \mathfrak{S}_{(2)} \; \mathfrak{T}_{(5)} \; \mathfrak{R}_{(3)} \\ \mathfrak{R}_{(4)} \; \mathfrak{S}_{(0)} \; \mathfrak{T}_{(2)} \end{pmatrix} = \begin{pmatrix} \beta_2 \beta_3 \beta_4 \beta_5 \beta_0 \beta_1 \gamma_5 \gamma_0 \gamma_1 \gamma_2 \gamma_3 \gamma_4 \alpha_3 \alpha_4 \alpha_5 \alpha_0 \alpha_1 \alpha_2 \\ \alpha_4 \alpha_5 \alpha_0 \alpha_1 \alpha_2 \alpha_3 \beta_0 \beta_1 \beta_2 \beta_3 \beta_4 \beta_5 \gamma_2 \gamma_3 \gamma_4 \gamma_5 \gamma_0 \gamma_1 \end{pmatrix}$$

und daraus

(13) $Q = (\alpha_4, \beta_2, \gamma_1, \alpha_2, \beta_0, \gamma_5, \alpha_0, \beta_4, \gamma_3) \, (\alpha_5, \beta_3, \gamma_2, \alpha_3, \beta_1, \gamma_0, \alpha_1, \beta_5, \gamma_4)$.

In diesem Falle ist

$$\pi_\varrho = -1, \; \pi_\sigma = 2, \; \pi_\tau = 3;$$

also haben die Zahlen

$$\pi_\varrho + \pi_\sigma + \pi_\tau = 4$$

und

$$a = 6$$

den grössten gemeinschaftlichen Divisor

$$\delta = 2;$$

mithin ist

$$\theta = 3.$$

Wenn wir hier von dem Cyclus z. B. $\mathfrak{S}$ die Form

$$(\beta_2, \beta_3, \beta_4, \beta_5, \beta_0, \beta_1)$$

oder

$$(\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5)$$

als die in der Substitution P befindliche annehmen, so treten die Elemente dieses Cyclus in den Cyclen der Substitution Q in den Reihen

$$\beta_2, \beta_0, \beta_4,$$
$$\beta_3, \beta_1, \beta_5$$

auf. Diese Reihen sind nicht die Reihen der Elemente des Cyclus $\mathfrak{S}$, wenn wir auch dieselben als cyclische ansehen. — Der Werth (13) genügt in der That der linearen und symbolischen Gleichung

$$QP = PQ$$

oder

$$QPQ^{-1} = P.$$

Bezeichnen wir nämlich die Complexion, welche aus der Substitution P nach Weglassung der Klammern und Kommata entsteht, mit A,

$$A = \alpha_4 \alpha_5 \alpha_0 \alpha_1 \alpha_2 \alpha_3 \beta_0 \beta_1 \beta_2 \beta_3 \beta_4 \beta_5 \gamma_2 \gamma_3 \gamma_4 \gamma_5 \gamma_0 \gamma_1,$$

und führen in dieser die Substitution

$Q = (\alpha_4, \beta_2, \gamma_1, \alpha_2, \beta_0, \gamma_5, \alpha_0, \beta_4, \gamma_3) \, (\alpha_5, \beta_3, \gamma_2, \alpha_3, \beta_1, \gamma_0, \alpha_1, \beta_5, \gamma_4)$

aus, so erhalten wir

$$QA = \beta_2 \beta_3 \beta_4 \beta_5 \beta_0 \gamma_0 \gamma_5 \gamma_1 \gamma_2 \gamma_3 \gamma_4 \alpha_3 \alpha_4 \alpha_5 \alpha_0 \alpha_1 \alpha_2,$$

und daraus laut Regel

$QPQ^{-1} = (\beta_2, \beta_3, \beta_4, \beta_5, \beta_0, \beta_1) \, (\gamma_5, \gamma_0, \gamma_1, \gamma_2, \gamma_3, \gamma_4) \, (\alpha_3, \alpha_5, \alpha_0, \alpha_1, \alpha_2)$,

was identisch ist mit

$$QPQ^{-1} = (\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5)(\gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_0, \gamma_1)(\alpha_4, \alpha_5, \alpha_0, \alpha_1, \alpha_2, \alpha_3)$$
$$= (\alpha_4, \alpha_5, \alpha_0, \alpha_1, \alpha_2, \alpha_3)(\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5)(\gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_0, \gamma_1) = P.$$

13. Die von Cauchy aufgestellte Regel zur Bildung von permutablen Substitutionen ist nicht, wie derselbe behauptet, allgemein. Auf Grund des vorher Gesagten, genügt es nämlich, um eine Substitution, die gegen eine regelmässige Substitution permutabel ist, zu bilden, nicht immer, die Tafeln (6) in θ andere mit h verticalen und k horizontalen Zeilen zu zergliedern

$$\left.\begin{matrix} \left\{\begin{matrix} \alpha, & \beta, & \gamma, & \dots \\ \alpha', & \beta', & \gamma', & \dots \\ \alpha'', & \beta'', & \gamma'', & \dots \\ & \text{etc.} & & \end{matrix}\right. \\[1ex] \left\{\begin{matrix} \lambda, & \mu, & \nu, & \dots \\ \lambda', & \mu', & \nu', & \dots \\ \lambda'', & \mu'', & \nu'', & \dots \\ & \text{etc.} & & \end{matrix}\right. \\[1ex] \left\{\begin{matrix} \varphi, & \chi, & \psi, & \dots \\ \varphi', & \chi', & \psi', & \dots \\ \varphi'', & \chi'', & \psi'', & \dots \\ & \text{etc.} & & \end{matrix}\right. \\ \text{etc.} \end{matrix}\right\} \quad (14)$$

und aus diesen, indem man „à la suite les unes des autres" die in denselben verticalen oder horizontalen Zeilen stehenden Elemente nimmt, die Cyclen

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \dots,$$

respective

$$\mathfrak{U}, \mathfrak{V}, \mathfrak{W}, \dots$$

zu bilden.*)

Ebenfalls nicht allgemein gültig ist die von Cauchy angegebene Methode zur Bildung der Substitution

$$\Theta = P^h = Q^k, \tag{15}$$

d. h. des Productes aller Circularfactoren

$$\left\{\begin{matrix} (\alpha, \lambda, \varphi, \dots)(\beta, \mu, \chi, \dots)(\gamma, \nu, \psi, \dots)\dots \\ (\alpha', \lambda', \varphi', \dots)(\beta', \mu', \chi', \dots)(\gamma', \nu', \psi', \dots)\dots \\ \text{etc.} \end{matrix}\right.$$

(Substitution der Ordnung θ), welche gemäss seiner Regel entsteht, indem man als Elemente der partiellen Cyclen „à la suite les unes

*) „Exerc." p. 214, 217. „Comp. rend." p. 1194, 1195.

des autres" die in den Tafeln (14) symmetrisch angeordneten Elemente nimmt.*)

Das Beispiel in Art. 12 giebt als Werth (13) für Q eine Substitution, deren Elemente sich in folgende, den Tafeln (14) ähnliche Tafeln

$$(\mathrm{p})\begin{cases}\alpha_4,\ \beta_2,\ \gamma_1\\ \alpha_5,\ \beta_3,\ \gamma_2\end{cases}$$

$$(\mathrm{q})\begin{cases}\alpha_2,\ \beta_0,\ \gamma_5\\ \alpha_3,\ \beta_1,\ \gamma_0\end{cases}$$

$$(\mathrm{r})\begin{cases}\alpha_0,\ \beta_4,\ \gamma_3\\ \alpha_1,\ \beta_5,\ \gamma_4\end{cases}$$

zergliedern lassen. Die verticalen Zeilen dieser Tafeln bilden dann die Cyclen der Substitution P, wenn wir die Elemente der Zeilen nicht in der Reihe der Tafeln

(p), (q), (r); v. (q), (r), (p); v. (r), (p), (q),

sondern in der Reihe

(p), (r), (q); v. (q), (p) (r); v. (r), (q), (p)

nehmen.

Auch das Product

$$\begin{cases}(\alpha_4,\ \alpha_0,\ \alpha_2)\ (\beta_2,\ \beta_4,\ \beta_0)\ (\gamma_1,\ \gamma_3,\ \gamma_5)\\ (\alpha_5,\ \alpha_1,\ \alpha_3)\ (\beta_3,\ \beta_5,\ \beta_1)\ (\gamma_2,\ \gamma_4,\ \gamma_0),\end{cases}$$

oder das Product

$$\begin{cases}(\alpha_0,\ \alpha_2,\ \alpha_4)\ (\beta_0,\ \beta_2,\ \beta_4)\ (\gamma_1,\ \gamma_3,\ \gamma_5)\\ (\alpha_1,\ \alpha_3,\ \alpha_5)\ (\beta_1,\ \beta_3,\ \beta_5,\ (\gamma_0,\ \gamma_2,\ \gamma_4),\end{cases}$$

d. h. die Substitution Θ, welche die Relation

$$\Theta = \mathrm{P}^k = \mathrm{Q}^h$$

ausdrücken soll, genügt nicht dieser Relation, und entsteht nicht, wenn wir als Elemente der Cyclen die in den Tafeln (p), (q), (r) symmetrisch angeordneten Elemente „à la suite les unes des autres" nehmen. Denn, obgleich hier

$$h = 3,\ k = 2,$$

so ist dennoch

$$\mathrm{Q} = \mathrm{P}^2 = \mathrm{Q}^6.$$

14. In der Folgerung**), welche dem Falle, dass die Substitution

$$\mathrm{P} = \mathfrak{P}$$

auf einen Cyclus,

$$h = 1,$$

*) „Exerc." p. 215. „Comp. rend." p. 1198.

**) „Comp. rend." p. 1199. „Exerc." p. 221.

reducirt wird, entspricht, ist nach dem Character der Substitution Θ

$$Q = P^k.$$

Hier bestimmt die Zahl k nicht die Anzahl der Cyclen der Substitution Q, sondern zeigt, dass der erhaltene Werth für Q eine Potenz des einzelnen Cyclus ist, welcher die Substitution P bildet. Wenn wir verschiedene Formen der Substitution P einführen, so können wir für k auch Zahlen erhalten, die zu a, der Anzahl der Elemente der Substitutionen P und Q, prim sind.

Ist

$$P = \mathfrak{R}\mathfrak{S}\mathfrak{T}\ldots$$

und soll Q nicht in Folge einer cyclischen Translocation der Cyclen

$$(\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots),$$

sondern durch cyclische Versetzung in den partiellen Substitutionen

$$\begin{pmatrix} \mathfrak{R}_{(\varrho_0)} & \mathfrak{S}_{(\sigma_0)} & \mathfrak{T}_{(\tau_0)} \\ \mathfrak{R}_{(\varrho_1)} & \mathfrak{S}_{(\sigma_1)} & \mathfrak{T}_{(\tau_1)} \end{pmatrix}$$

erhalten werden, so findet sich

$$Q = \mathfrak{R}^{\pi_\varrho} \mathfrak{S}^{\pi_\sigma} \mathfrak{T}^{\pi_\tau} \ldots,$$

wo jede der Zahlen

$$\pi_\varrho, \pi_\sigma, \pi_\tau, \ldots$$

irgend einen von den Werthen

$$0, 1, 2, \ldots, a-1$$

annehmen kann.

15. Wenn wir jetzt den Fall, dass

$$a = 1,$$

berücksichtigen, so wird

$$\pi_\varrho = \pi_\sigma = \pi_\tau = \ldots = 0,$$

und die Cyclen

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

reduciren sich auf Cyclen der ersten Ordnung, d. h. sie sind unversetzbare Elemente der Substition P. Bei Berücksichtigung dieser Elemente wird sich die Anzahl der aus der Gleichung

$$QP = PQ$$

für Q erhaltenen Werthe um einen der Anzahl der Substitutionen, welche wir aus diesen Elementen bilden können, gleichen Factor vergrössern*). Da nun aber derselbe sich auf

$$1 . 2 . 3 \ldots h$$

reducirt und ferner nach der Formel (Art. 2)

*) „Exerc." p. 222, 223. „Comp. rend." p. 1192.

$$\omega = (1.2\ldots f)(1.2\ldots g)\ldots a^f b^g \ldots{}^{*}),$$

die Anzahl der mit P ähnlichen durch die Existenz von h Cyclen erster Ordnung hervorgerufenen Formen, gleich dem Factor

$$1.2.3\ldots h.1^h$$

ist, so können wir die in P vorkommenden Cyclen erster Ordnung als solche betrachten, die in P eine regelmässige Substitution bilden. Wir haben also nicht mehr nöthig, uns mit diesen Elementen in den allgemeinen Lehrsätzen, wie es Cauchy thut, zu beschäftigen, nachdem wir am Anfange jeder Herleitung uns vorbehalten haben, dass man alle diese Elemente zum Vorschein bringen dürfe.

§ III.

16. J. A. Serret nennt die permutablen Substitutionen „échangeables“ und behandelt sie in seinem Werke**) in dem Capitel „Des substitutions échangeables entre elles“. Ist in der Gleichung

$$ST = TS$$

die gegebene Substitution S ein Product der regelmässigen Substitionen

$$S = PP'P''\ldots,$$

so modificirt Serret, um eine mit P permutable und durch cyclische Versetzung der μ Cyclen entstandene partielle Substitution zu bilden, die zweite, dritte etc. partielle Complexion durch Versetzung der Colonnen der Art, dass er in der unteren Zeile dieselben Complexionen, die in den vorhergehenden Theilen der oberen Zeile sich befanden, erhält. Es ist dann:

$$Q = \begin{pmatrix} C_1\ C_2 \ldots C_{\mu-1}\ C_0' \\ C_0\ C_1 \ldots C_{\mu-2}\ C_{\mu-1} \end{pmatrix},$$

und C_0, sowie C_0' sind dabei dieselben, oder von einander verschiedene Formen der in dem Cyclus (C_0) befindlichen Complexionen. Man kan die partiellen Complexionen folgendermassen darstellen

$$\begin{aligned} C_0 &= a_0 a_1 \ldots a_{i-1}, \\ C_1 &= b_0 b_1 \ldots b_{i-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ C_{\mu-1} &= f_0 f_1 \ldots f_{i-1}. \end{aligned}$$

Mit Hilfe des so erhaltenen Q, sowie der aus P′, P″ etc. gewonnenen Q′, Q″ etc. bildet man

$$T = QQ'Q''\ldots.$$

---

*) „Exerc.“ T. III. p. 192. „Comp. rend.“ T. XXI. p. 1192.

**) „Cours d'algèbre supérieure.“ (3ème édit.) Tome II. nos. 403—409.

Ist die Complexion C_0' von der Form

$$C_0' = a_\varrho\, a_{\varrho+1} \ldots a_{\varrho+i-1},$$

so erhält Serret für die einzelnen Cyclen der Substitution Q die Werthe

$$(G_0), (G_1), \ldots, (G_{\varrho-1}),$$

deren Anzahl i beträgt, wenn $\varrho = 0$, d. h. $C_0 = C_0''$ ist.

17. Da nun ϱ den Werth jeder Zahl der Reihe

$$0, 1, 2, \ldots, i-1$$

annehmen kann, da ferner λ die Anzahl der aus jedem Cyclus (C_ξ) der Substitution P genommenen Elemente bezeichnet, so ist [obgleich die Anzahl j der Elemente jedes Cyclus (G_ξ) immer den Werth $\lambda\mu$ hat] für den Fall, dass ϱ zu i prim, oder kein Divisor der Zahl i ist, weder

$$\lambda\mu\varrho$$

die Anzahl der in der Substitution Q befindlichen Elemente, noch

$$i = \lambda\varrho\,^*).$$

Bildet man die Tafel

$$\begin{array}{l} a_\xi,\ a_{\xi+1}, \ldots, a_{\xi+\varrho-1}, \\ b_\xi,\ b_{\xi+1}, \ldots, b_{\xi+\varrho-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f_\xi,\ f_{\xi+1}, \ldots, f_{\xi+\varrho-1}, \end{array} \qquad (16)$$

und bezeichnet die aus den Elementen der horizontalen Zeilen entstandenen Complexionen mit

$$\mathfrak{A}_\xi, \mathfrak{B}_\xi, \ldots, \mathfrak{F}_\xi,$$

ferner die aus den Elementen der verticalen Zeilen hervorgegangenen mit

$$\mathfrak{M}_\xi, \mathfrak{M}_{\varrho+1}, \ldots, \mathfrak{M}_{\xi+\varrho-1},$$

so ist es, obgleich die Complexionen der Cyclen der Substitution Q sich folgendermassen darstellen lassen

$$\begin{array}{l} G_0 = \mathfrak{M}_\varrho\ \mathfrak{M}_{2\varrho} \ldots \mathfrak{M}_{(\lambda-1)\varrho}, \\ G_1 = \mathfrak{M}_{\varrho+1}\ \mathfrak{M}_{2\varrho+1} \ldots \mathfrak{M}_{(\lambda-1)\varrho+1}, \\ \text{etc.} \end{array}$$

1° nicht unbedingt nöthig, dass die Anzahl der Cyclen der Substitution Q gleich ϱ ist, denn sie kann kleiner sein; 2° lassen sich die Complexionen der Cyclen der Substitution P nicht immer folgendermassen darstellen

$$\begin{array}{l} C_0 = \mathfrak{A}_0\ \mathfrak{A}_\varrho\ \mathfrak{A}_{2\varrho} \ldots \mathfrak{A}_{(\lambda-1)\varrho}, \\ C_1 = \mathfrak{B}_0\ \mathfrak{B}_\varrho\ \mathfrak{B}_{2\varrho} \ldots \mathfrak{B}_{(\lambda-1)\varrho}, \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ C_{\mu-1} = \mathfrak{F}_0\ \mathfrak{F}_\varrho\ \mathfrak{F}_{2\varrho} \ldots \mathfrak{F}_{(\lambda-1)\varrho}; \end{array}$$

*) p. 239.

3⁰ bewährt sich daher nicht immer die Formel

(17) $$[(C_0)(C_1)\ldots(C_{\mu-1})]^\varrho = [(G_0)(G_1)\ldots(G_{\varrho-1})]^\mu\text{ *)},$$

sollten wir auch unter ϱ die Anzahl der Cyclen der Substitution Q verstehen.

18. In dem Beispiel des Art. 12 haben wir unter den Voraussetzungen, welche uns zu dem Werthe (13) der Substitution Q führen und mit Benutzung der Bezeichnung

$$\alpha_0 = a_0,\text{ etc.};\ \beta_4 = b_0,\text{ etc.};\ \gamma_3 = c_0,\text{ etc.},$$

auszuführen

$$\begin{pmatrix} C_1\, C_2\, C_0 \\ C_0\, C_1\, C_2 \end{pmatrix} = \begin{pmatrix} b_0\, b_1\, b_2\, b_3\, b_4\, b_5\, c_0\, c_1\, c_2\, c_3\, c_4\, c_5\, a_4\, a_5\, a_0\, a_1\, a_2\, a_3 \\ a_0\, a_1\, a_2\, a_3\, a_4\, a_5\, b_0\, b_1\, b_2\, b_3\, b_4\, b_5\, c_0\, c_1\, c_2\, c_3\, c_4\, c_5 \end{pmatrix}.$$

Hier ist

$$\mu = 3,\ \varrho = 4,\ i = 6,$$

und wir kommen auf a_0 zurück, nachdem wir aus jedem Cyclus drei Elemente genommen haben; es ergiebt sich also

$$\lambda = 3.$$

Daraus folgt

$$\begin{aligned} \lambda\varrho &= 12 = 2i \\ \lambda\varrho\mu &= 36 = 2i\mu. \end{aligned}$$

Aus der Tafel

$$\begin{matrix} a_\xi,\ a_{\xi+1},\ a_{\xi+2},\ a_{\xi+3}, \\ b_\xi,\ b_{\xi+1},\ b_{\xi+2},\ b_{\xi+3}, \\ c_\xi,\ c_{\xi+1},\ c_{\xi+2},\ c_{\xi+3}, \end{matrix}$$

haben wir

$$\begin{aligned} G_0 &= \mathfrak{M}_0\, \mathfrak{M}_\varrho\quad \mathfrak{M}_{2\varrho}, \\ G_1 &= \mathfrak{M}_1\, \mathfrak{M}_{\varrho+1}\, \mathfrak{M}_{2\varrho+1}; \end{aligned}$$

die Anzahl dieser Cyclen beträgt also hier nicht ϱ, sondern 2, und 2ϱ, $2\varrho+1$ sind die kleinsten positiven Reste dieser Zahlen nach dem Modul i, obgleich sie nach der Tafel (16) kleiner als i sein sollten. Die Complexionen

$$C_0,\ C_1,\ C_2$$

lassen sich nicht durch totale Wiederholungen der Complexionen, welche die entsprechenden horizontalen Zeilen bilden, ausdrücken. Ausserdem ist, wenn wir auch unter ϱ die Anzahl der Cyclen der Substitution Q, d. h. 2, verstehen,

$$P^\varrho = [Q^\mu]^2.$$

---

*) p. 240, 241.

§ IV.

19. Die aufzustellende Substitution Q entsteht, indem man über eine gewisse Form der Substitution

$$P = (C_0)(C_1)\dots(C_m)$$

eine andere schreibt, bei welcher die Translocation einer gewissen Zahl ihrer Cyclen durch die cyclische Versetzung

$$((C_0), (C_1), \dots, (C_{\mu-1})) \tag{18}$$

ausgedrückt werden kann. Die auf diese Weise erhaltene Substitution wird ihre Bedeutung nicht verändern, wenn man die Colonnen so versetzt, dass der erste Theil der die untere Zeile bildenden Complexion die partielle Complexion

$$C_0 = a_0 a_1 a_2 \dots a_{n-1}$$

liefert. Man hat dann in der oberen Zeile

$$C_1 = b_{\varrho_1} b_{\varrho_1+1} \dots b_{\varrho_1+n-1},$$

wobei unter jeder Zahl $\varrho_1 + \xi$ der kleinste positive Rest nach dem Modul n zu verstehen ist. Versetzt man die folgenden Colonnen der Art, dass sich in der unteren Zeile C_1 neben C_0 befindet, etc., bis man endlich in der unteren Zeile die in dem vorhergehenden Theile der oberen Zeile auftretende Complexion $C_{\mu-1}$ erhält, so wird mau über derselben die Complexion

$$C_0' = a_\varrho a_{\varrho+1} a_{\varrho+2} \dots a_{\varrho+n-1}$$

finden.

In der Substitution

$$\begin{pmatrix} C_1 \, C_2 \, . \, . \, . \, C_{\mu-1} \; C_0' \\ C_0 \, C_1 \, C_2 \; . \, . \, . \; C_{\mu-1} \end{pmatrix} \tag{19}$$

haben die ersten Elemente der Cyclen

$$C_1, C_2, \dots, C_{\mu-1}, C_0',$$

d. h.

$$b_{\varrho_1}, c_{\varrho_2}, \dots, f_{\varrho_{\mu-1}}, a_\varrho$$

beliebige Zahlen aus der Reihe

$$0, 1, 2, \dots, n-1,$$

als Indices. Durch diese Bezeichnung ergeben sich alle n^μ Werthe (Art. 4), während die Bezeichnung in Art. 16 nur n Werthe zugelassen hat.

20. Da die Complexionen der Cyclen

$$(C_1), (C_2), (C_3), \dots, (C_{\mu-1})$$

der Substitution (19) in den beiden Zeilen einförmig sind, so lässt sich nach der vorgelegten Darstellungsmethode die Frage, ob nach der

Herausnahme der Elemente der Cyclus sich abschliesst oder nicht, sowie welche Elemente und in welcher Reihenfolge dieselben man aus dem ersten Cyclus (C_0) und dem folgenden nehmen soll, durch die Substitution ad hoc

$$\begin{pmatrix} C_0' \\ C_0 \end{pmatrix}$$

d. h.

$$\begin{pmatrix} a_\varrho & a_{\varrho+1} & a_{\varrho+2} \dots a_{\varrho+n-1} \\ a_0 & a_1 & a_2 \quad \dots a_{n-1} \end{pmatrix}$$

vollständig beantworten.

Um den Cyclus (G_ξ) zu schliessen, werden wir aus dem ersten und den folgenden Cyclen soviel Elemente nehmen, bis die Anzahl λ der aus (C_0) genommenen Elemente, der Congruenz

$$\xi + \lambda\varrho \equiv (\text{mod } n),$$

d. h.

(20) $$\lambda\varrho \equiv 0 \ (\text{mod } n),$$

genügt. Die Zahl ϱ ist gegeben, oder richtiger gesagt, sie ist durch die Formen, welche wir den Cyclen in (19) willkürlich geben können, bestimmt; von dieser Zahl hängt also λ ab. Wir können in der Congruenz (20) für die Zahl ϱ, entsprechend dem Modul n, drei Fälle unterscheiden:

1° ϱ ist zu n prim,
2° ϱ ist ein Divisor von n,
3° ϱ und n haben den grössten gemeinschaftlichen Divisor δ.

Wenn ϱ zu n prim ist, so wird die Zahl λ der Relation (20) für

$$\lambda = n$$

genügen. Folglich werden in diesem Falle, um einen Cyclus der Substitution Q zu bilden, alle Elemente aus den ersten, so wie auch aus den folgenden Cyclen der Substitution P genommen. Die Substitution Q ist also eine cyclische Substitution von μn Elementen.

Wenn ϱ ein Divisor von n ist, dann bestimmt die Congruenz (20)

$$\lambda = \frac{n}{\varrho}$$

und dieselbe geht in die Gleichheit

$$n = \lambda\varrho$$

über. Zur Bildung des Cyclus (G_ξ) werden aus dem ersten Cyclus sowie aus dem folgenden Cyclen der Substitution P, je λ Elemente genommen. Die Anzahl ν der Elemente des Cyclus (G_ξ) hat also dann den Werth

$$\nu = \mu\lambda.$$

Wenn wir hier von dem Elemente α_ξ, $\xi < \varrho$, ausgehen und der Reihe nach

$$\alpha_\xi,\ b_{\varrho_1+\xi},\ c_{\varrho_2+\xi},\ \ldots,\ f_{\varrho_{\mu-1}+\xi},\ a_{\xi+\varrho},\ b_{\varrho_1+\xi+\varrho},\ \ldots$$

nehmen, so sind alle Indices kleiner als n, und die Aufeinanderfolge, in welcher wir diese Elemente aus jedem Cyclus herausgreifen, ist dieselbe, in welcher sie sich in diesen Cyclen befinden. Da kein Element, das zwischen den Elementen mit den Indices ξ und $\xi + \varrho$, $\xi + \varrho$ und $\xi + 2\varrho$, etc. vorkam, zur Bildung des Cyclus (G_ξ) genommen wurde, so kann ξ jeden von den ϱ Werthen

$$0, 1, 2, \ldots, \varrho - 1$$

annehmen und die Substitution Q hat ϱ Cyclen.

Ist ϱ zu n prim, so können wir nur dann die Elemente in der Reihenfolge, in welcher dieselben in den Cyclen der Substitution P vorkommen, herausnehmen, wenn

$$\varrho = 1.$$

22. Besitzen aber allgemein ϱ und n den grössten gemeinschaftlichen Divisor δ, indem

$$n = \chi\delta,$$
$$\varrho = \psi\delta,$$

so verwandelt sich die Congruenz (20) in folgende

$$\lambda\psi \equiv 0 \pmod{\chi}. \qquad (21)$$

Hier ist ψ zum Modul prim; die Zahl λ kann der letzten Congruenz mit dem Werthe

$$\lambda = \chi$$

genügen; es folgt daher

$$n = \lambda\delta = \frac{\lambda\varrho}{\psi}.$$

Sonach wird sich die Aufgabe laut (21) auf diejenige, bei welcher ψ zu χ, der Zahl der zu nehmenden Elemente, prim ist, zurückführen lassen. Wir nehmen demgemäss zur Bildung des Cyclus (G_ξ) alle die Elemente, deren Indices um ein Multiplum der Zahl δ von einander differiren. In dem Cyclus (C_0) giebt es vor $a_{\xi+\varrho}$ ψ solcher Elemente, d. h.

$$a_\xi,\ a_{\xi+\delta},\ a_{\xi+2\delta},\ \ldots,\ a_{\xi+(\psi-1)\delta};$$

von dem letzten ab, bis zu $a_{\xi+2\varrho}$ (wenn $\xi + 2\varrho < n$), u. s. w. finden sich deren ebenso viel. Wir können also dem ξ nur einen von den Werthen

$$0, 1, 2, \ldots, \delta - 1$$

beilegen. Bezeichnet σ die Anzahl der Cyclen der Substitution Q, so ist

$$\sigma = \delta.$$

In jedem der Cyclen kommen

$$\nu = \mu\lambda$$

Elememente vor.

Allgemein gültig ist die Formel für die Zahl λ der aus jedem Cyclus genommenen Elemente,

$$\lambda = \frac{n\psi}{\varrho},$$

sowie für die Zahl der Cyclen der Substitution Q

$$\sigma = \frac{\varrho}{\psi}.$$

Ebenso erhält man

$$\psi - 1$$

für die Anzahl der Elemente des Cyclus der Substitution P, welche zu demselben Cyclus gehören und zwischen solchen Elementen vorkommen, deren Indices um ϱ von einander differiren. Diese Formeln können auch auf die zwei vorherbesprochenen Fälle bezogen werden. Denn in dem ersten, bei welchem wir

$$\varrho = \psi$$

annehmen, folgt

$$\lambda = n,\ \sigma = 1,\ \varrho - 1;$$

in dem zweiten ergiebt sich, vermöge

$$\psi = 1,$$

$$\lambda = \frac{n}{\varrho},\ \sigma = \varrho,\ 0.$$

23. Wir sehen daraus, dass, wenn wir die Tafel der Elemente mit σ verticalen und μ horizontalen Zeilen bilden

$$(22)\quad \left\{\begin{array}{lllll} a_{\xi}, & a_{\xi+1}, & a_{\xi+2}, & \ldots, & a_{\xi+\delta-1}, \\ b_{\varrho_1+\xi}, & b_{\varrho_1+\xi+1}, & b_{\varrho_1+\xi+2}, & \ldots, & b_{\varrho_1+\xi+\delta-1}, \\ c_{\varrho_2+\xi}, & c_{\varrho_2+\xi+1}, & c_{\varrho_2+\xi+2}, & \ldots, & c_{\varrho_2+\xi+\delta-1}, \\ \multicolumn{5}{l}{\dotfill,} \\ f_{\varrho_{\mu-1}+\xi}, & f_{\varrho_{\mu-1}+\xi+1}, & f_{\varrho_{\mu-1}+\xi+2}, & \ldots, & f_{\varrho_{\mu-1}+\xi+\delta-1}, \end{array}\right.$$

oder allgemeiner

$$(23)\quad \left\{\begin{array}{lllll} a_{\xi}, & a_{\xi+1}, & a_{\xi+2}, & \ldots, & a_{\xi+\frac{\varrho}{\psi}-1}, \\ b_{\varrho_1+\xi}, & b_{\varrho_1+\xi+1}, & b_{\varrho_1+\xi+2}, & \ldots, & b_{\varrho_1+\xi+\frac{\varrho}{\psi}-1}, \\ c_{\varrho_2+\xi}, & c_{\varrho_2+\xi+1}, & c_{\varrho_2+\xi+2}, & \ldots, & c_{\varrho_2+\xi+\frac{\varrho}{\psi}-1}, \\ \multicolumn{5}{l}{\dotfill,} \\ f_{\varrho_{\mu-1}+\xi}, & f_{\varrho_{\mu-1}+\xi+1}, & f_{\varrho_{\mu-1}+\xi+2}, & \ldots, & f_{\varrho_{\mu-1}+\xi+\frac{\varrho}{\psi}-1}, \end{array}\right.$$

und ihre horizontalen Zeilen mit

$$\mathfrak{A}_{\varrho},\ \mathfrak{B}_{\varrho_1+\xi},\ \mathfrak{C}_{\varrho_2+\xi},\ \dots,\ \mathfrak{F}_{\varrho_{\mu-1}+\xi},$$

und die verticalen mit

$$\mathfrak{M}_{\xi},\ \mathfrak{M}_{\xi+1},\ \mathfrak{M}_{\xi+2},\dots,\ \mathfrak{M}_{\xi+\frac{\varrho}{\psi}-1}$$

bezeichnen, die Complexionen der Cyclen sich folgendermassen darstellen lassen

$$\begin{array}{lllll}
C_0 = \mathfrak{A}_0 & \mathfrak{A}_{\frac{\varrho}{\psi}} & \mathfrak{A}_{2\frac{\varrho}{\psi}} & \dots & \mathfrak{A}_{n-\frac{\varrho}{\psi}}, \\
C_1 = \mathfrak{B}_{\varrho_1} & \mathfrak{B}_{\varrho_1+\frac{\varrho}{\psi}} & \mathfrak{B}_{\varrho_1+2\frac{\varrho}{\psi}} & \dots & \mathfrak{B}_{\varrho_1+n-\frac{\varrho}{\psi}}, \\
\dots\dots & & & & \\
C_{\mu-1} = \mathfrak{F}_{\varrho_{\mu-1}} & \mathfrak{F}_{\varrho_{\mu-1}+\frac{\varrho}{\psi}} & \mathfrak{F}_{\varrho_{\mu-1}+2\frac{\varrho}{\psi}} & \dots & \mathfrak{F}_{\varrho_{\mu-1}+n-\frac{\varrho}{\psi}},
\end{array}$$

und

$$\begin{array}{lllll}
G_0 = \mathfrak{M}_0 & \mathfrak{M}_{\varrho} & \mathfrak{M}_{2\varrho} & \dots & \mathfrak{M}_{n\psi-\varrho}, \\
G_1 = \mathfrak{M}_1 & \mathfrak{M}_{\varrho+1} & \mathfrak{M}_{2\varrho+1} & \dots & \mathfrak{M}_{n\psi-\varrho+1}, \\
\dots\dots & & & & \\
G_{\frac{\varrho}{\psi}-1} = \mathfrak{M}_{\frac{\varrho}{\psi}-1} & \mathfrak{M}_{2\frac{\varrho}{\psi}-1} & \mathfrak{M}_{3\frac{\varrho}{\psi}-1} & \dots & \mathfrak{M}_{n\psi-\varrho+\frac{\varrho}{\psi}-1}.
\end{array}$$

Man hat hierbei unter allen Indices, welcher grösser als n sind, die kleinsten positiven Reste nach dem Modul n zu verstehen. So ist z. B. der Index des letzten $\mathfrak{M}$, d. h.

$$n\psi - \varrho + \frac{\varrho}{\psi} - 1 = (\lambda - 1)\varrho + \frac{\varrho}{\psi} - 1,$$

die Zahl

$$n - \varrho + \frac{\varrho}{\psi} - 1 = n - (\psi - 1)\frac{\varrho}{\psi} - 1.$$

Ferner ist

$$Q = (G_0)\ G_1) \dots (G_{\frac{\varrho}{\psi}-1}).$$

Jede von den Complexionen (G_{ξ}) ist aus $\frac{\varrho}{\psi}$ entsprechenen $\mathfrak{M}_{\xi}$, d. h. aus der entsprechenden verticalen Zeile der Tafel (22) oder der Tafel (23) entstanden.

Diese Tafeln werden, wenn

$$\delta = \varrho, \text{ d. h. } \psi = 1,$$

auf die Tafel (16), und wenn man noch die horizontalen Zeilen gegen die verticalen vertauscht, auf eine von den Tafeln (14) zurückgeführt. Sie dienen also auch für den Fall, wo ϱ ein Divisor des n ist.

Ist ϱ zu n prim, also

$$\delta = 1, \text{ d. h. } \psi = \varrho,$$

dann werden die Tafeln (22) und (23) auf eine Colonne (nämlich auf die erste) reducirt.

24. Wir erhalten die Substitution von der Ordnung λ

$$(24)\quad Q = \begin{cases} \left(a_0, a_{\frac{\varrho}{\psi}}, \ldots, a_{(\lambda-1)\frac{\varrho}{\psi}}\right)\left(a_1, a_{\frac{\varrho}{\varphi}+1}, \ldots, a_{(\lambda-1)\frac{\varrho}{\psi}+1}\right)\cdots \\ \qquad\qquad \left(a_{\frac{\varrho}{\psi}-1}, a_{2\frac{\varrho}{\psi}-1}, \ldots, a_{n-1}\right) \\ \left(b_{\varrho_1}, b_{\varrho_1+\frac{\varrho}{\varphi}}, \ldots, b_{\varrho_1+(\lambda-1)\frac{\varrho}{\psi}}\right)\cdots\left(b_{\varrho_1+\frac{\varrho}{\psi}-1}, b_{\varrho_1+2\frac{\varrho}{\psi}-1}, \ldots, b_{\varrho_1-1}\right) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \left(f_{\varrho_{\mu-1}}, f_{\varrho_{\mu-1}+\frac{\varrho}{\psi}}, \ldots, f_{\varrho_{\mu-1}+(\lambda-1)\frac{\varrho}{\psi}}\right)\cdots \\ \qquad\qquad \left(f_{\varrho_{\mu-1}+\frac{\varrho}{\psi}-1}, f_{\varrho_{\mu-1}+2\frac{\varrho}{\psi}-1}, \ldots, f_{\varrho_{\mu-1}-1}\right) \end{cases}$$

aus der Substitution

$$(C_0)\,(C_1)\,(C_2)\ldots(C_{\mu-1}),$$

deren Cyclen $n = \lambda\frac{\varrho}{\psi}$ Elemente haben, indem wir diese letzte Substitution zur Potenz $\frac{\varrho}{\psi}$ erheben. Dabei treten die Elemente der Cyclen von Θ in derselben Reihenfolge auf, in welcher sie in den Cyclen der Substitution P vorkommen.

Wenn wir die Substitution Q, die von der Ordnung $\nu = \mu\lambda$ ist, zur Potenz μ erheben, so erhalten wir eine Substitution Θ_1 von der Ordnung λ. Da wir jedoch die Elemente zur Bildung der Cyclen (G_ξ) nicht immer in derselben Reihe, in welcher sie in den Cyclus der Substitution P aufeinanderfolgen, genommen haben, so wird die Substitution Θ_1 nur unter gewissen Bedingungen mit der Substitution Θ übereinstimmen. Zur Bildung des Cyclus (G_ξ) haben wir aus dem Cyclus (C_0) die Elemente mit den Indices

$$\xi, \xi+\varrho, \xi+2\varrho, \ldots, \xi+(\chi-1)\varrho$$

d. h.

$$\xi, \xi+\psi\delta, \xi+2\psi\delta, \ldots, \xi+(\chi-1)\psi\delta$$

genommen. Mit denselben Indices und in derselben Reihenfolge befinden sich die Elemente in dem entsprechenden Cyclus der Substitution Θ_1. Von diesen Elementen ist das zweite in dem entsprechenden Cyclus der Substitution Θ dasjenige, dessen Index $\xi + x\psi\delta$ der Relation

$$\xi + x\psi\delta \equiv (\xi+\delta) \pmod{n}$$

genügt; mithin

$$x\psi\delta \equiv \delta \pmod{\chi\delta},$$

und

$$x\psi \equiv 1 \pmod{\chi}.$$

Da ψ zu χ prim ist, ergiebt sich

$$x = \frac{1+\varphi\chi}{\psi},$$

wobei wir unter φ die kleinste ganze Zahl verstehen, die für den Werth von x eine ganze Zahl liefert. Folglich erhalten wir Θ, indem wir die Substitution Θ_1 zur Potenz x erheben. Es wird also

$$\Theta = \left[(C_0)\,(C_1)\ldots(C_{\mu-1})\right]^{\frac{\varrho}{\psi}} = \left[(G_0)\,(G_1)\ldots(G_{\frac{\varrho}{\psi}-1})\right]^{\mu\frac{1+\varphi\chi}{\psi}}. \quad (25)$$

Dies ist die allgemeine Bedingung, welcher zwei aus denselben Elementen entstandene Substitutionen genügen müssen (Art. 1), damit für die letzteren die, durch die lineare und symbolische Gleichung

$$QP = PQ$$

ausgedrückte Relation stattfinde.

Die Substitution Θ hat

$$\mu\frac{\varrho}{\psi}$$

Cyclen, d. h. so viel, als sich Elemente auf der Tafel (22) oder (23) befinden. Wenn wir uns vorstellen, dass wir alle Tafeln (22) ausschreiben, nachdem wir statt δ der Reihe nach

$$\delta,\ 2\delta,\ 3\delta, \ldots, (\chi-1)\,\delta$$

genommen, oder alle Tafeln (23), nachdem in ihnen statt $\frac{\varrho}{\psi}$ der Reihe nach

$$\frac{\varrho}{\psi},\ 2\frac{\varrho}{\psi},\ 3\frac{\varrho}{\varphi}, \ldots, (\chi-1)\frac{\varrho}{\psi}$$

gesetzt worden, so bilden die Elemente, welche in diesen Tafeln symmetrisch, d. h. in den Kreuzungspunkten derselben horizontalen und verticalen Zeilen vorkommen, nach der Reihe der Tafeln genommen, die Cyclen der Substitution Θ.

Wenn wir in (24) und (25)

$$\psi = 1$$

nehmen, dann ist

$$\varphi = 0,\ \frac{1+\varphi\chi}{\psi} = 1,$$

und aus (25) erhalten wir für den Fall, wo φ ein Divisor des n ist,

$$[(C_0)\,(C_1)\ldots(C_{\mu-1})]^{\varrho} = [(G_0)\,(G_1)\ldots(G_{\varrho-1})]^{\mu},$$

d. h. die Formel (17). Und wenn darin

$$\mu = m,$$

so ergiebt sich

$$\Theta = P^{\varrho} = Q^{m},$$

d. h. die Formel (15).

Setzt man in (24) und (25)

$$\varrho = \psi,$$

dann ist

$$\chi = n,$$

$$\Theta = (C_0)(C_1)(C_2)\ldots(C_{\mu-1}) = \left[(G_0)\right]^{\mu\frac{1+\varphi n}{\varrho}},$$

und zwar ist Θ nur aus den ersten Elementen jeder horizontalen Zeile der Tafeln zusammengesetzt.

25. In dem oben (Art. 12, 13, 18) angeführten Beispiele ist, wenn wir den Werth (13) suchen, laut Art. 19,

$$\begin{aligned} C_0 &= a_0 a_1 a_2 a_3 a_4 a_5, \\ C_1 &= b_4 b_5 b_0 b_1 b_2 b_3, \\ C_2 &= c_2 c_3 c_4 c_5 c_2 c_1, \\ C_0' &= a_4 a_5 a_0 a_1 a_1 a_2. \end{aligned}$$

Vermöge

$$\begin{pmatrix} C_0' \\ C_0 \end{pmatrix}$$

haben wir

$$n = 6,\ \varrho = 4,\ \psi = 2,\ \lambda = \chi = 3,\ \sigma = \delta = 2.$$

Bilden wir die Tafel

$$\begin{cases} a_\xi &, a_{\xi+1}, \\ b_{4+\xi}, & b_{5+\xi}, \\ c_{3+\xi}, & c_{4+\xi}, \end{cases}$$

so ist

$$n - \frac{\varrho}{\psi} = 4,\ n\psi - \varrho \equiv 2 \pmod 6;$$

also

$$\begin{aligned} C_0 &= \mathfrak{A}_0\, \mathfrak{A}_2\, \mathfrak{A}_4, \\ C_1 &= \mathfrak{B}_4\, \mathfrak{B}_0\, \mathfrak{B}_2, \\ C_2 &= \mathfrak{C}_3\, \mathfrak{C}_5\, \mathfrak{C}_1, \end{aligned}$$

und

$$\begin{aligned} G_0 &= \mathfrak{M}_0\, \mathfrak{M}_4\, \mathfrak{M}_2, \\ G_1 &= \mathfrak{M}_1\, \mathfrak{M}_5\, \mathfrak{M}_3; \end{aligned}$$

mithin

$$Q = (G_0)(G_1).$$

Da

$$\frac{\varrho}{\psi} = 2,\ \varphi = 1,\ \frac{1+\varphi\chi}{\psi} = 2,\ \mu = 3,$$

so ist

$$\Theta = P^2 = Q^6.$$

Sei ferner

$$P = (C_0)(C_1)(C_2)\, C_3)(C_4)\, C_5)(C_6).$$

Zur Aufstellung des Werthes von Q, der durch Versetzung z. B. der fünf ersten Cyclen nach dem Schema

$$((C_0)(C_1)(C_2)(C_3)(C_4))$$

entsteht (hier ist also $m = 7$, $\mu = 5$), hat man beispielsweise

$$n = 16,\ \varrho_1 = 13,\ \varrho_2 = 0,\ \varrho_3 = 8,\ \varrho_4 = 3,\ \varrho = 12$$

zu setzen und erhält unter dieser Annahme, vermöge

$$\begin{pmatrix} C_0' \\ C_0 \end{pmatrix},$$

die Werthe

$$\psi = 3,\ \lambda = \chi = 4,\ \sigma = \delta = 4.$$

Man hat sonach die Tafel

$$\begin{cases} a_{\xi}\ , a_{\xi+1}\ , a_{\xi+2}\ , a_{\xi+3}\ , \\ b_{13+\xi}, b_{14+\xi}, b_{15+\xi}, b_{16+\xi}, \\ c_{\xi}\ , c_{\xi+1}\ , c_{\xi+2}\ , c_{\xi+3}\ , \\ d_{8+\xi}\ , d_{9+\xi}\ , d_{10+\xi}, d_{11+\xi}, \\ e_{3+\xi}\ , e_{4+\xi}\ , e_{5+\xi}\ , e_{6+\xi}\ . \end{cases}$$

Aus ihr folgt laut Regel

$$\begin{aligned} C_0 &= \mathfrak{A}_0\ \mathfrak{A}_4\ \mathfrak{A}_8\ \mathfrak{A}_{12}, \\ C_1 &= \mathfrak{B}_{13}\ \mathfrak{B}_1\ \mathfrak{B}_5\ \mathfrak{B}_9\ , \\ C_2 &= \mathfrak{C}_0\ \mathfrak{C}_4\ \mathfrak{C}_8\ \mathfrak{C}_{12}, \\ C_3 &= \mathfrak{D}_8\ \mathfrak{D}_{12}\ \mathfrak{D}_0\ \mathfrak{D}_4\ , \\ C_4 &= \mathfrak{E}_3\ \mathfrak{E}_7\ \mathfrak{E}_{11}\ \mathfrak{E}_{15}, \end{aligned}$$

und

$$\begin{aligned} G_0 &= \mathfrak{M}_0\ \mathfrak{M}_{12}\ \mathfrak{M}_8\ \mathfrak{M}_4, \\ G_1 &= \mathfrak{M}_1\ \mathfrak{M}_{13}\ \mathfrak{M}_9\ \mathfrak{M}_5, \\ G_2 &= \mathfrak{M}_2\ \mathfrak{M}_{14}\ \mathfrak{M}_{10}\ \mathfrak{M}_6, \\ G_3 &= \mathfrak{M}_3\ \mathfrak{M}_{15}\ \mathfrak{M}_{11}\ \mathfrak{M}_7; \end{aligned}$$

mithin

$$Q = (G_0)\,(G_1)\,(G_2)\,(G_3).$$

Da

$$\frac{\varrho}{\psi} = 4,\ \varphi = 2,\ \frac{1+\varphi\chi}{\psi} = 3,$$

so ist

$$\Theta = [(C_0)(C_1)(C_2)(C_3)(C_4)]^4 = [(G_0)(G_1)(G_2)(G_3)]^{15}.$$